UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Docket No. 20-cr-40036-TSH
v.	)	
	)	***LEAVE TO FILE UNDER SEAL***
	)	***AND TO FILE REDACTED***
VINCENT KIEJZO	)	***MEMORANDUM GRANTED ON***
	)	***1/4/2023***
	)	

DEFENDANT'S SUPPLEMENTAL MEMORANDUM IN SUPPORT OF HIS MOTION TO SUPPRESS AND MOTION TO RECONSIDER DENIAL OF MOTION TO COMPEL

Defendant, Vincent Kiejzo, submits this supplemental memorandum to his previously filed Motion to Suppress (D.E. # 172) and also moves this Court to reconsider its denial of Mr. Kiejzo's motion to compel (D.E. # 117 and 157). Since the filing of Mr. Kiejzo's Motion to Suppress, undersigned counsel discovered new information relevant to both his motion to suppress and his motion to compel. This information reveals the broader scope of the international investigation at issue in this case. It shows not just the depth and nature of the United States' involvement in the investigation, but critical U.S. involvement at an earlier stage than previously represented by the government, and thus provides additional support for the defendant's arguments in his Motion to Suppress and his previously-denied discovery requests.

After oral argument on Mr. Kiejzo's Motion to Suppress was held in late October 2022, undersigned counsel learned through independent investigation that the foreign country in which the server hosting both Website 2 and Website 3 was located was [redacted]. News reports and government press releases about the identification and eventual seizure of that server reveal two key things: (1) years before receiving any "tip" regarding IP addresses from a foreign law enforcement agency ("FLA") in this case, the FBI was significantly involved in the international

investigation that led to both the identification and seizure of the server in [redacted], and (2) finding that server, shutting it down, and de-anonymizing the IP addresses that had visited the target sites was clearly a joint venture and operation between the U.S. and other countries' FLAs. This goes to the very heart of American involvement and collaboration with FLAs and lends further support to Mr. Kiejzo's request for a *Franks* hearing.

Sometime in 2017, an international collaboration between INTERPOL, Europol, and law enforcement agencies in [redacted] The FBI and [redacted]

[1] [redacted]

[2] [redacted]

[3] *Id.*

[4] [redacted]

[5] *Id.*

[redacted] were integral to this operation. First, the FBI helped [redacted] law enforcement locate the IP address of the individual hosting the server.[6] Next, the [redacted] then monitored the internet traffic associated with that IP address and determined that it was being used not merely as a user but as a server or relay node.[7] The FBI then used a deanonymization technique to corroborate the identification of the server on the Tor network.[8] This investigation thus contained not just multiple stages, but multiple actors who shared information and acted in concert with each other.

With the critical investigation techniques and efforts by both the FBI and [redacted] authorities were able to determine that the server was run by [redacted] law enforcement [redacted] seized the server in June 2019.[10] The government has never disclosed any information related to that search and seizure (even refusing to name the FLA and country where the server was hosted). And most importantly, the government has never made any assurances whatsoever that the investigation, the search, or the seizure of the server comported with basic U.S. Constitutional standards and the rule of law applied in the U.S. Ultimately, [redacted] affirmatively shared and provided materials from that seizure to both the FBI and [redacted].[11] Shortly thereafter, [redacted] shared with other countries the IP addresses that had visited the sites hosted on the server.[12]

To date, the government has never disclosed – either to the defense or to the magistrate who issued the search warrant in this case – the fact, the timeline, or the scope of U.S. involvement in the investigation, search, seizure, and review of materials obtained from [redacted], and

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

instead has repeatedly denied what is now obvious: that the U.S. was not simply a passive participant or recipient of information here. It is now clear that U.S. law enforcement worked hand in hand with other countries to not only identify the administrators of the Tor hidden websites allegedly visited in Mr. Kiejzo's case ([redacted]), but also to identify and take down the server that hosted those websites. Failing to include the extent to which U.S. law enforcement was engaged in this joint venture to investigate the target websites in Mr. Kiejzo's case was a significant and material omission. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012); *see also United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (finding that the defendant had made a *prima facie* showing, for purposes of motion to compel discovery, that the joint venture doctrine applied and that malware had been used to obtain the defendant's IP address where U.S. law enforcement worked with Australian and New Zealand authorities to uncover IP addresses in the United States).

Finally, it appears that the government is in fact in possession of information about the methodology used to de-anonymize the IP addresses in this investigation. In a case stemming from the same investigation, the government filed a complaint on the public docket that "outlined the law enforcement methodology used to unearth defendant's criminal conduct." *See* Government's Motion to Seal the Complaint, *United States v. Kidder*, No. 1:21-cr-00118-LJV (W.D.N.Y. Mar. 16, 2020), ECF No. 7 (attached as Exhibit B). Realizing the complaint contained "information that could reveal highly-sensitive law enforcement methods," the government then moved to seal the complaint. *Id*. Undersigned counsel have not accessed or viewed the unredacted complaint. *See* Redacted Complaint, *United States v. Kidder*, No. 1:21-cr-00118-LJV (W.D.N.Y. Mar. 16, 2020), ECF No. 9 (attached as Exhibit C). However, the government's Motion to Seal in *Kidder*

undermines the repeated assertions by the government in this case that the government has no knowledge of the methodology used in this investigation.

For the above reasons, and those stated in his Motion to Suppress, this Court should suppress all evidence and fruits obtained pursuant to the invalid search warrant and grant Mr. Kiejzo a *Franks* hearing. Additionally, this Court should reconsider its denial of Mr. Kiejzo's Motion to Compel. At the absolute minimum, Mr. Kiejzo has made a *prima facie* showing of the joint venture such that he is entitled to further discovery on these issues. *See Mitrovich*, 458 F. Supp. 3d at 966-67.

Respectfully submitted,
VINCENT KIEJZO
By His Attorney,

/s/ Sandra Gant
Sandra Gant, BBO # 680122
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

/s/ Caitlin Jones
Caitlin Jones, MN ID # 0397519
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on January 4, 2023.

/s/ Sandra Gant
Sandra Gant